BCSE 309L

ASSIGNMENT – 9

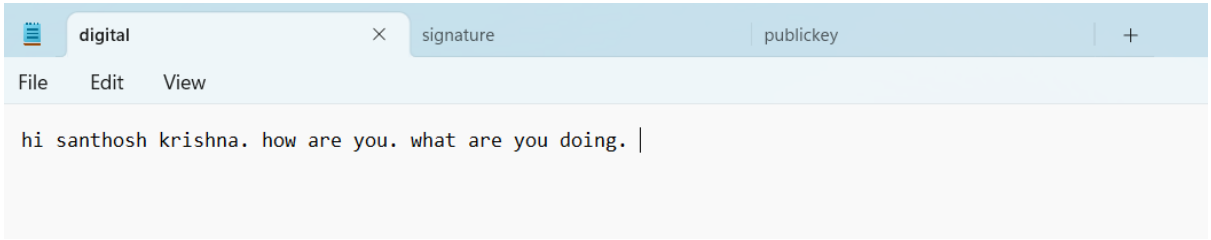
SANTHOSH KRISHNA R

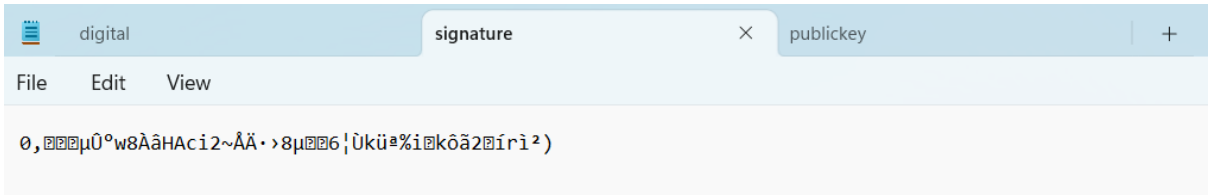
21BCE1651

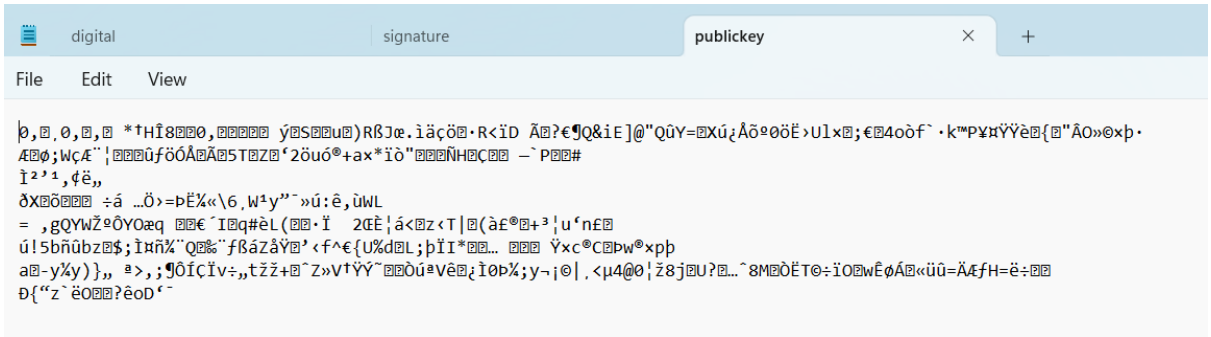
```
import java.io.*;
import java.security.*;

class Main {
    public static void main(String args[]) {
        if (args.length != 1) {
            System.out.println("Usage: nameOfFileToSign");
            return;
        }

        try {
            KeyPairGenerator keyGen = KeyPairGenerator.getInstance("DSA",
"SUN");
            SecureRandom random = SecureRandom.getInstance("SHA1PRNG", "SUN");
            keyGen.initialize(1024, random);
            KeyPair pair = keyGen.generateKeyPair();
            PrivateKey priv = pair.getPrivate();
            PublicKey pub = pair.getPublic();

            Signature dsa = Signature.getInstance("SHA1withDSA", "SUN");
            dsa.initSign(priv);

            try (FileInputStream fis = new FileInputStream(args[0]);
                 BufferedInputStream bufin = new BufferedInputStream(fis)) {
                byte[] buffer = new byte[1024];
                int len;
                while ((len = bufin.read(buffer)) >= 0) {
                    dsa.update(buffer, 0, len);
                }
            }

            byte[] realSig = dsa.sign();

            try (FileOutputStream sigfos = new
FileOutputStream("signature.txt")) {
```

```
                sigfos.write(realSig);
            }

            byte[] key = pub.getEncoded();
            try (FileOutputStream keyfos = new
FileOutputStream("publickey.txt")) {
                keyfos.write(key);
            }
        } catch (Exception e) {
            System.err.println("Caught exception " + e.toString());
        }
    }
}
```

```
PS C:\Users\SANTHOSH> cd Desktop
PS C:\Users\SANTHOSH\Desktop> javac Main.java
PS C:\Users\SANTHOSH\Desktop> java Main digital.txt
```








```
0,□,0,□,□ *†HÎ8□□0,□□□□□ ý□S□□u□)RßJœ.ìäçö□·R<ïD Ã□?€¶Q&iE]@"QûY=□Xú¿Åõº0öË›Ul×□;€□4oòf`·k™P¥¤ŸŸè□{□"ÂO»©×þ·
Æ□ø;WçÆ¨¦□□□ûƒöÓÅ□Ã□5T□Z□‘2öuó®+a×*ïò"□□□Ñ H□Ç□□ —`P□□#
ì²’¹,¢ë„
ðX□õ□□□ ÷á …Ö›=Þ£¼«\6¸W¹y”¯»ú:ê,ùWL
= ,gQYWŽºÔYOæq □□€´I□q#èL(□□·Ï  2Œè¦á<□z‹T|□(à£®□+³¦u‘n£□
ú!5bñûbz□$;Ìж¾¨Q□‰¨ƒßáZåŸ□’‹f^€{U%d□L;þÏI*□□… □□□ Ÿ×c®C□Þw®×pþ
a□-y¾y)}„ ª>,;¶ÔÍÇÏv÷„tžž+□ˆZ»V†ŸÝ˜□□Òúª Vê□¿Ì0Þ¾;y¬¡©|¸<µ4@0¦ž8j□U?□…ˆ8M□ÒËT©÷ïO□wÊøÁ□«üû=ÄÆƒH=ë÷□□
Ð{“z`ëO□□?èoD‘¯
```